DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents
July 4 - 31, 2011

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064443	Missing/Stolen Equipment	VISN 06 Asheville, NC	7/6/2011	8/8/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/6/2011	INC000000159174	N/A	N/A	N/A		

Incident Summary

A Dell Optiplex computer was reported missing on 06/30/11 at approximately 2:00 PM. The mobile videoconference (MOVI) camera that had been installed on the PC was also gone. The keyboard and mouse were still in the room. The PC was last seen by an OIT staff member. It was acquired on 02/16/10. The inventory lists and National On-line Information System (NOIS) tickets are currently being searched for additional information.

Incident Update

07/07/11:
According to the Information Security Officer (ISO), the workstation was last seen on 06/30/11 and was located in a mulit-purpose room that is used by Veterans/Patients for meetings but has to be unlocked for use. It is not believed that the workstation contained personally identifiable information (PII) or protected health information (PHI) due to the fact that the workstation is used for presentations only. There are also Microsoft Group Policies in place that prevent users from saving information to the hard drive and the users' "My Documents" folder is mapped to a secure server. There are cameras in the area and the VA Police are in the process of reviewing the video footage.

07/12/11:
The CPU and camera have not been located but the Police have reviewed the video from the camera and saw a person of interest but the person turned in the opposite direction of the camera. Police are currently checking with the individual who held the AA class in the room that evening.

07/22/11:
The Chief of Police stated that he cannot definitively identify the individual from the video.

Resolution

The facility installed new locks on the doors, placed locks on the PC and monitor and placed the computer in a locked cabinet. In addition, new procedures now control access to the room.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064472	Mishandled/ Misused Physical or Verbal Information	VISN 08 Orlando, FL	7/6/2011	7/11/2011	High

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/6/2011	INC000000159305	N/A	N/A	N/A	1	

Incident Summary

A Prosthetics technician provided Veteran A's wife with a brief, hand-written description of the proper chair lift she was to purchase. When she returned home with her husband, she turned over the note and discovered it was written on the backside of Veteran B's consultation sheet. The wife returned the consultation sheet to the Director's Office on her husband's next appointment. The Prosthetics Chief has been notified and they are attempting to identify the originator of the note. The note contained Veteran B's name, address, date of birth, full SSN and protected health information (PHI).

Incident Update

07/07/11:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 71 Mis-Handling incidents this reporting period. Because of repetition, the other 70 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The Prosthetics technician was verbally counseled by the Prosthetics supervisor. In addition, the Privacy Officer has been invited to review this incident at the Department's next scheduled training meeting in August. All members have already been cautioned about this incident.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064477	Mishandled/ Misused Physical or Verbal Information	VISN 15 Kansas City, MO	7/6/2011		High

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/6/2011	INC000000159335	N/A	N/A	N/A		1

Incident Summary

Veteran A called to report receiving a package of medication in the mail that he had not ordered. Veteran A is not getting medications from this medical center or being actively seen as a patient at this time. Veteran A's name and correct address were on the outside of package. Veteran A was asked to open the package to relay the medication information. Veteran A verified that the label on the bottle had his name on it. By cross referencing the prescription number, it was found the medication was for Veteran B who has the exact same name but different last 4 digits of the SSN. Veteran A had not taken any medication from this package and was directed not to. Veteran A stated he was on the way back to the medical center to return the medication and the entire package to the Pharmacy.

Incident Update

07/07/11:
Veteran B will be sent a notification letter.

NOTE: There were a total of 70 Mis-Mailed incidents this reporting period. Because of repetition, the other 69 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064555	Mishandled/ Misused Physical or Verbal Information	VISN 15 St Louis, MO	7/8/2011		High

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	N/A	N/A	N/A	N/A	N/A	1	

Incident Summary

The deceased Veteran A's daughter contacted the St. Louis VAMC claiming to have Veteran B's discharge instructions in her possession. She indicated that she would only return the documents if the VA was willing to forgive her father's medical bills and that she had contacted local news media. She contacted the Information Security Officer (ISO) at the Marion VAMC during the Privacy Officer's (PO) absence. She was asked to return the documents. To date, no documents have been returned to either the Marion VAMC or the St. Louis VAMC. No Release of Information (ROI) requests have been completed or received since August 2010 during which the request was only that a placard form be completed. Discharge instruction forms were verified in Vista Imaging as belonging to correct Veteran. NOTE: The decision was made to open this ticket despite the lack of evidence to support an actual incident.

Incident Update

07/19/11:
The Southern Illinoisan reporter contacted the facility Office of Public and Intergovernmental Affairs (OPIA) to verify information that he researched on the HIPAA website. Veteran A's daughter has not yet returned information belonging to Veteran B. The PO will attempt to contact her again. The reporter provided the name of Veteran B, whose information was allegedly compromised. The PO contacted Veteran B to discuss the issue and offer credit monitoring. Veteran B told the PO that deceased Veteran A's daughter had contacted him.

07/20/11:
The PO spoke with Veteran A's daughter via telephone. The PO asked the daughter to return the original document as well as any copies that may have been produced. She stated the documents will be placed in the mail by the end of this week.

07/26/11:
No documents have been received at either facility. The POs at both facilities have been unable to contact the daughter.

08/08/11:
The deceased Veteran A's daughter still has not returned the documents. The Marion PO is not aware of any news article or report as of this date. Veteran B will receive a letter offering credit protection services.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064584	Missing/Stolen Equipment	VISN 07 Montgomery, AL	7/11/2011	8/5/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/11/2011	INC000000159995	N/A	N/A	N/A		

Incident Summary

Several pieces of equipment were not located during the June inventory for Central Alabama Veterans Health Care System Montgomery Campus.

Incident Update

07/11/11:
The following equipment was not located during the June inventory for Montgomery: 4 BlackBerry devices, 8 laptops, 3 Dell workstations and one IPAQ Smart Phone. The laptops are encrypted but the computers are not. The BlackBerry devices are password enabled and do not have email capability. None of the equipment is currently on the network. Staff continues to search for this equipment.

NOTE: There were a total of 6 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 5 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

The IT Operations Manager has summarized the corrective actions and goals taking place at the facility aimed at preventing lost IT inventory incidents:

1. Reduce overall inventory by 4% or more (371 items) before 09/30/11. They have already turned in nearly 200 items.
2. Organize the storage areas into "current inventory" and "awaiting disposal" separated areas.
3. Created a hand receipt in VistA IT module for BlackBerry devices, cell phones, laptops, thumb drives, and other equipment that is loaned out to users for off-campus activities.
4. Users will be responsible for maintaining an electronically signed hand receipt. Users will be responsible for electronically signing before the equipment leaves IT possession. Technicians will be checking to ensure hand receipts are current when they return ticketed items to users and also ensure the hand receipts are terminated
5. Assign technicians sections of the 2 campuses and the Community Based Outpatient Clinics (CBOC) for a rotating inventory. Rotation will be on a 90 or 120 day rotation.
6. Reduce access to storage area down to 4 keys per campus - 2 technician and 2 managers. Doors will be locked when the inventory manager is not in the storage area
7. Technicians will return equipment to the inventory managers prior to receiving new equipment
8. Procedures were communicated to all IT customer service staff on 08/04/11.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064591	Missing/Stolen Equipment	VISN 05 Baltimore, MD	7/11/2011	8/4/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/11/2011	INC000000160036	N/A	N/A	N/A		

Incident Summary

A Picture Archiving and Communications Systems (PACS) workstation was stolen. The PC, monitor, keyboard, and cables were taken. While users are told not to store information on the hard drive, the facility is confirming that this policy was followed.

Incident Update

07/18/11:
The workstation is still missing. The Imaging Service contacted the employees who use the workstation and requested verbal confirmation that no information was saved to the hard drive of the PC. All employees responded to the inquiry and all said they did not save any VA data or information, sensitive or non-sensitive, to the hard drive of the PC. The VA Police have reviewed recordings of exit areas, but have not identified any suspicious activity. Imaging and Information Resource Management (IRM) will evaluate whether the reading room PCs, which are medical devices, can be encrypted.

Resolution

Users confirmed that no information was stored on the hard drive. The workstation has not been located. OIG discussed the incident with the Associate Medical Center Director. Since no information was stored on the hard drive, OIG took no further action.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064678	Unauthorized Electronic Access	VISN 16 New Orleans, LA	7/13/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/13/2011	INC000000160524	N/A	N/A	N/A		

Incident Summary

Upon arrival to her locked office, a VA workforce member found that her computer was logged on with her email up and running. She also stated that her file cabinet was unlocked and open. The workforce member stated that she logged off the network yesterday at approximately 3:30 PM before going home. The workforce member is looking to see if any information or files are missing.

Incident Update

07/18/11:
The IT staff is still looking at the Active Directory log. The office was locked and there is no protected health information (PHI) missing. This incident is still under investigation,

07/26/11:
After a review, the office door was locked upon the arrival to the office. VA Police Service has not started a Police report due to the office being locked upon the workforce member's arrival to the office. The Privacy Office (PO) has yet to forward all of the information from her review to the Information Security Officer (ISO) Group, who is working with management for a copy of the PO's review. The ISO has also not received the Information Resource Management log report yet.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064817	Missing/Stolen Material (Non-Equipment)	VISN 16 Little Rock, AR	7/19/2011		High

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/19/2011	INC000000161459	N/A	N/A	N/A	449	

Incident Summary

A VA volunteer printed an inpatient listing for 07/18/11, left the office area and came back in a few minutes. The volunteer had covered the information but did not lock it up as policy states. This listing was missing when the volunteer returned.

Incident Update

07/26/11:
Four hundred and forty nine (449) patients will receive letters offering credit protection services, due to full names and full SSNs being exposed.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000064863	Missing/Stolen Equipment	VISN 16 Jackson, MS	7/20/2011	7/26/2011	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/20/2011	NC000000161704	N/A	N/A	N/A		

Incident Summary

A laptop located in the Research department was reported missing. This laptop does not contain any personally identifiable information (PII) or protected health information (PHI). It was only used to run the electroporator/electrofusion apparatus that does not generate any patient data. This device is only used every couple of months and it was last used around 06/10/11. The Research department is located behind badge entry doors and the swipe list has been generated and passed on to the VA Police service.

Incident Update

07/19/11:
The laptop is not encrypted due to the fact that it is part of a medical instrument that modifies cells connected to a piece of Research equipment. There is no PII/PHI on the laptop.

Resolution

This equipment was not a piece of VA equipment. It contained zero PII/PHI and was used to stimulate cells connected to a piece of Research equipment. This was reported to the VA Police Service and the OIG was notified. The Research department is behind badge entry doors and the door log was turned over to the VA Police service.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065041	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Tucson, AZ	7/25/2011	8/5/2011	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/26/2011	INC000000162963	N/A	N/A	N/A		1

Incident Summary

Patient A received a Medline Industries medical supply intended for Patient B. Patient B's name and type of medical supply was compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Tucson Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a Medline packing error. The packing error has been reported to Medline for investigation and corrective action.

Incident Update

07/26/11:
Patient B will receive a letter of notification.

NOTE: There were a total of 6 Mis-Mailed CMOP incidents out of 5,928,407 total packages (8,934,154 total prescriptions) mailed out for this reporting period. Because of repetition, the other 5 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Resolution

The packing error has been reported to Medline for investigation and corrective action. They have responded that employee will be retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
SPE000000065091	Missing/Stolen Equipment	VISN 23 Minneapolis, MN	7/26/2011		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
	7/26/2011	INC000000163083	N/A	N/A	N/A		

Incident Summary

Three laptops were secured in room 2B106 waiting to be imaged by IRM personnel. A Technician noticed they were missing. An extensive search was done and the laptops were not found. These laptops were new and had never been put into service. No sensitive data was on the devices.

Incident Update

07/26/11:
No data breach occurred. The laptops were new and had never been imaged or used on the VA network. This ticket will remain on the Daily Incident Report and the Monthly Report to Congress as it pertains to missing/stolen equipment.

Total number of Lost Blackberry Incidents	21
Total number of Internal Un-encrypted E-mail Incidents	96
Total number of Mis-Handling Incidents	71
Total number of Mis-Mailed Incidents	70
Total number of Mis-Mailed CMOP Incidents	6
Total number of IT Equipment Inventory Incidents	6
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	6 (5 encrypted)